UNITED STATES PATENT AND TRADEMARK OFFICE

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/811,719 | 03/29/2004 | Michael A. Rothman | 42P18654 | 1421 |

7590          04/28/2008
Anthony H. Azure
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

| EXAMINER |
|---|
| HOANG, DANIEL L |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/28/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 10/811,719 | ROTHMAN ET AL. |
| | Examiner | Art Unit | |
| | DANIEL L. HOANG | 2136 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on <u>15 January 2008</u>.

2a)☒ This action is **FINAL**.     2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) <u>1-30</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-30</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

## DETAILED ACTION

## RESPONSE TO ARGUMENTS

Applicant's arguments in regards to claim 1 and similar independent claims have been considered but are not persuasive.

Applicant argues that it is incorrect to combine the references, Lettvin and Ho. Applicant argues this due to the fact that Lettvin allegedly executes anti-virus software before the operating system executes while Ho teaches an anti-virus scanning module with an operating system. Examiner respectfully disagrees. The Ho reference was relied upon in the previous action to teach the claimed limitation of a "virus signature database." While it is true that the anti-virus scanning module taught by Ho is used with an operating system, it does not mean that the anti virus database comprising a plurality of computer virus signatures requires an operating system to be loaded in order to be accessible. It is certainly possible for the database to be accessed prior to loading of an operating system. Because of this, it is perfectly feasible to combine the teachings of Lettvin with Ho in order for the anti virus software taught by Lettvin to access the virus signature database taught by Ho.


Applicant's arguments in regards to claim 27 have been considered but are not persuasive. Applicant argues that Ho does not teach a VMM as the operating system because the virtual scanning processor and virtual machine execute using a single operating system and does not use a separate operating system for each virtual monitor. Examiner respectfully disagrees. Applicant's current claim language of claim 27 does not recite a separate operating system for each virtual monitor. Thus the argument is moot.


## CLAIMS PRESENTED

**Claims 1-30 are presented.**

## CLAIM REJ2CTIONS

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claims 1-18, 20-25, and 27-30 are rejected under 35 U.S.C. 103(a) as being**

**unpatentable over Lettvin, US Patent No. 5826012, and further in view of Ho et al.,**

**US Patent No. 7188369.**

**As per claim 1, 12, 20:**

**Lettvin teaches:**

A method, comprising:

initializing a virus scanner during a pre-boot phase of a computer system;

 *[see col. 4, lines 62-67]*

scrubbing data read from an input/output (I/O) device of the computer system by the virus scanner [using

a virus signature database] before the data is loaded;  and

 *[see col. 8, lines 24-32]*

enacting a platform policy if a virus is detected in the data.

 *[see col. 8, lines 33-51]*

*Lettvin is not explicit in teaching that the virus scanner uses a virus signature database.  Ho teaches a*

*virus signature database (see figure 2, element 201).  It would have been obvious to one of ordinary skill*

*in the art to modify the invention taught by Lettvin to include a virus signature database.  One would be*

*motivated to do this in order to allow to system to use a plurality of virus signatures that can be*

*continuously updated and/or replaced (col. 1, lines 29-40).*

**As per claim 2, Lettvin teaches:**

The method of claim 1, further comprising scrubbing contents of a memory device of the computer system during the pre-boot phase by the virus scanner.

   *[see col. 8, lines 24-32]*


**As per claim 3, 13, Ho teaches:**

The method of claim 1, further comprising updating the virus signature database with updated virus signatures.

   *[see col. 1, lines 50-64]*

*One would be motivated to combine what is taught above by Ho with the Lettvin reference discussed above in order to detect newly occurring viruses which may not be present in outdated virus signatures.*


**As per claim 4, Ho teaches:**

The method of claim 3 wherein the virus signature database is updated during the pre-boot phase.

   *[see col. 1, lines 50-64]*

*One would be motivated to combine what is taught above by Ho with the Lettvin reference discussed above in order to detect newly occurring viruses ASAP.*


**As per claim 5, 14, Lettvin teaches:**

The method of claim 1 wherein the virus signature database is not exposed to an operating system executing on the computer system.

   *[see col. 3, lines 53-67]*


**As per claim 6, 22, Lettvin teaches:**

The method of claim 5 wherein the virus signature database is stored in a firmware-reserved area.

*[see col. 3, lines 53-67]*

## As per claim 7, 17, Ho teaches:

The method of claim 1 wherein the virus scanner is executing in a virtual machine monitor (VMM) executing on the computer system, the VMM supporting at least one virtual machine (VM) executing on the computer system, wherein the VM executes an operating system that is different from the VMM and the operating systems executed by other VMs.

*[see col. 5, lines 25-67]*

## As per claim 8, 18, Ho teaches:

The method of claim 7 wherein scrubbing data read from the I/O device includes: receiving a request from a requester to read data from the I/O device, the requester in a VM of the at least one VM; loading at least a portion of the requested data into a buffer; scrubbing the at least a portion of the requested data with the virus scanner; returning an error signal to the requester if the virus scanner detects a virus in the at least a portion of the requested data; and forwarding the requested data to the requester if the virus scanner does not detect a virus in the at least a portion of the requested data.

*[see figures 4 and 5]*

## As per claim 9, 15, 24, 28, Ho teaches:

The method of claim 1 wherein the virus scanner is operable during the pre-boot phase, an operating system (OS) runtime phase, and an after-life phase of the computer system independent of an operating system of the computer system.

*[see col. 4, lines 63-37 and col. 4, lines 1-2]*

*One would be motivated to combine the above teachings of Ho with the Lettvin reference discussed above in order to detect viruses during all phases of OS usage.*

**As per claim 10, 16, 25, 29, Lettvin teaches:**

The method of claim 1 wherein the virus scanner scrubs the data without having knowledge of a file

system of the data.

>    *[see col. 4, lines 62-67]*


**As per claim 11, Lettvin teaches:**

The method of claim 1, further comprising enacting the platform policy if the virus scanner detects non-

normal behavior within the computer system.

>    *[see col. 8, lines 24-32]*

**As per claim 21, Lettvin teaches:**

The computer system of claim 20, further comprising a network interface operatively coupled to the

processor, the virus scanner to scrub data read from the network interface using the virus signature

database before the data is loaded in the memory device.

>    *[see col. 3, lines 29-52]*


**As per claim 23, Ho teaches:**

The system of claim 20 wherein execution of the firmware instructions further perform operations

comprising updating the virus signature database with updated virus signatures downloaded from an

external virus signature repository communicatively coupled to the computer system.

>    *[see col. 5, lines 1-24]*

*Downloading the virus signatures from an external repository provides added security and less chance*

*that the data can be tampered with.*


**As per claim 27:**

A computer system, comprising:

a virtual machine monitor (VMM) to support at least one virtual machine (VM);

>   *[see Ho reference, col. 5, lines 25-67]*

an input/output (I/O) device, the VMM to emulate an I/O controller for the I/O device;

>   *[see Ho reference, col. 1, lines 50-64]*

a virus scanner within the VMM to scrub data read from the I/O device before the data is loaded;  and

>   *[see Lettvin reference, col. 8, lines 24-32]*

a virus signature database to facilitate identification of a virus by the virus scanner.

>   *[see Ho reference, figure 2, element 201]*


**Claims 19, 26, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lettvin and Ho as applied to claim 1 above, and further in view of Huntington et al., US Patent No. 6907524.**

**As per claim 19, 26, 30:**

The Lettvin and Ho references have been discussed above.  Lettvin and Ho are not explicit in teaching:

>   "The article of manufacture of claim 12 wherein the plurality of instructions to operate in
>
>   compliance an Extensible Firmware Interface (EFI) specification."

Huntington teaches a firmware substantially in compliance with the Extensible Firmware Interface (EFI) specification (col. 1, lines 51-55).  It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the methods disclosed by Lettvin and Ho to include what is taught by Huntington.  One would be motivated to do so in order to provide protection from viruses on computer systems that use an Extensible Firmware Interface (col. 1, lines 6-10).


**CONCLUSION**

>   **THIS ACTION IS MADE FINAL.**  Applicant is reminded of the extension of time policy as set forth

in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from

the mailing date of this action.  In the event a first reply is filed within TWO MONTHS of the mailing date

of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date the advisory action

is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action.  In no event, however, will the statutory period for reply expire later than SIX

MONTHS from the mailing date of this final action.

# POINTS OF CONTACT

*.      Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

> Commissioner for Patents
> P.O. Box 1450
> Alexandria, VA 22313-1450

> **Hand-delivered responses** should be brought to

> Customer Service Window
> Randolph Building
> 401 Dulaney Street
> Alexandria, VA 22314

*.      Any inquiry concerning this communication or earlier communications from the examiner should

be directed to Daniel L. Hoang whose telephone number is 571-270-1019.  The examiner can normally

be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Nasser Moazzami can be reached on 571-272-4195.  The fax phone number for the organization where

this application or proceeding is assigned is 571-273-8300.

> *Information regarding the status of an application may be obtained from the Patent Application
> Information Retrieval (PAIR) system.  Status information for published applications may be
> obtained from either Private PAIR or Public PAIR.  Status information for unpublished
> applications is available through Private PAIR only.  For more information about the PAIR system,
> see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR
> system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).*

/Daniel L. Hoang/

Examiner, Art Unit 2136


/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136